Institute for Theoretical Computer Science

Leibniz Universität Hannover

Complexity of Model Checking for Modal Dependence Logic

Johannes Ebbing
joint work with Peter Lohmann

Institut für Theoretische Informatik
Leibniz Universität Hannover

January 23, 2012

Overview

Motivation

What is the motivation for Modal Dependence Logic?

Motivation

What is the motivation for Modal Dependence Logic?

- Dependence atom extends ordinary modal logic

Motivation

What is the motivation for Modal Dependence Logic?

- Dependence atom extends ordinary modal logic
- CTL is used for verifying systems e.g. integrated circuits

Motivation

What is the motivation for Modal Dependence Logic?

- Dependence atom extends ordinary modal logic
- CTL is used for verifying systems e.g. integrated circuits
- MDL seen as first approach of DCTL (= CTL + dependence atom)

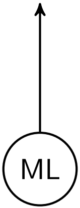
Motivation

What is the motivation for Modal Dependence Logic?

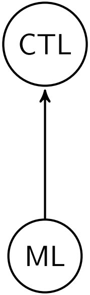
- Dependence atom extends ordinary modal logic
- CTL is used for verifying systems e.g. integrated circuits
- MDL seen as first approach of DCTL (= CTL + dependence atom)
- MDL is based on teams, not on single assignments / worlds

Introduction

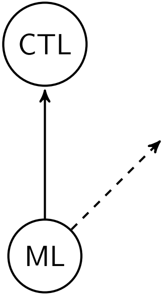
Introduction



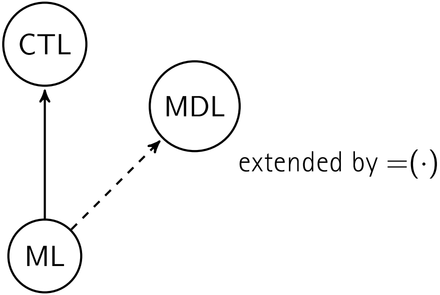
Introduction



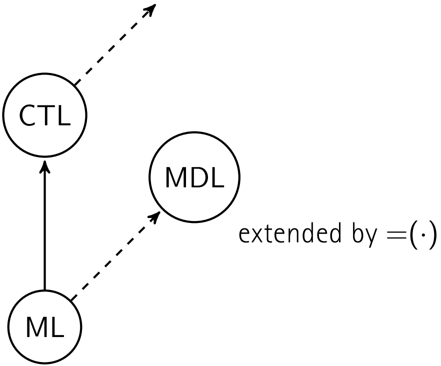
Introduction



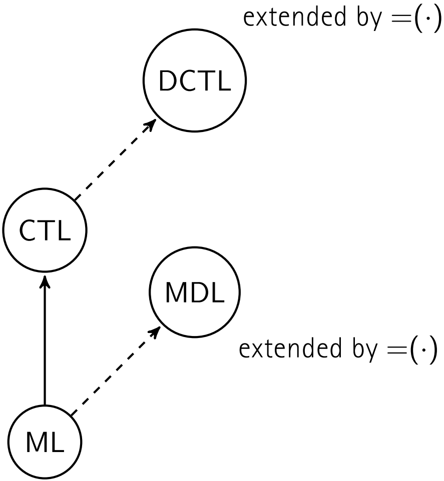
Introduction



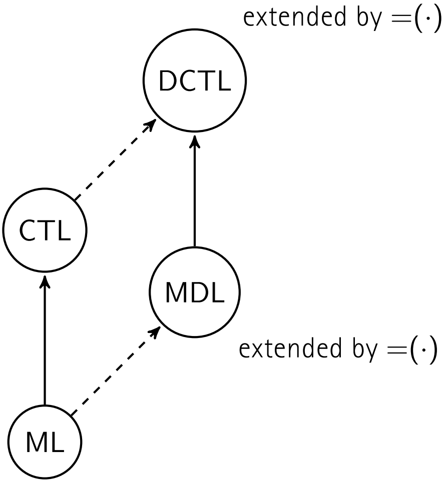
Introduction



Introduction



Introduction



Kripke structure

Definition

Kripke structure

Definition

A Kripke structure (or frame) over a set of atomic propositions AP (or AP-Kripke structure) is a tuple $W = (S, R, \pi)$, where

Kripke structure

Definition

A Kripke structure (or frame) over a set of atomic propositions AP (or AP-Kripke structure) is a tuple $W = (S, R, \pi)$, where

- $S \neq \emptyset$

Kripke structure

Definition

A Kripke structure (or frame) over a set of atomic propositions AP (or AP-Kripke structure) is a tuple $W = (S, R, \pi)$, where

- $S \neq \emptyset$
- $R \subseteq S \times S$

Kripke structure

Definition

A Kripke structure (or frame) over a set of atomic propositions AP (or AP-Kripke structure) is a tuple $W = (S, R, \pi)$, where

- $S \neq \emptyset$
- $R \subseteq S \times S$
- $\pi : S \to \mathcal{P}(AP)$

Kripke structure

Definition

A Kripke structure (or frame) over a set of atomic propositions AP (or AP-Kripke structure) is a tuple $W = (S, R, \pi)$, where

- $S \neq \emptyset$
- $R \subseteq S \times S$
- $\pi : S \to \mathcal{P}(AP)$

If $s \in S$, s is called world. We call S the set of worlds. R is called the transition relation between the worlds, and π is called the labeling function.

Modal Dependence Logic

Syntax of Modal Logic

Modal Dependence Logic

Syntax of Modal Logic

Let AP be a set of atomic propositions and $p_1, \ldots, p_n, q \in AP$. The syntax of modal logic formulae is defined by the grammar:

Modal Dependence Logic

Syntax of Modal Logic

Let AP be a set of atomic propositions and $p_1, \ldots, p_n, q \in AP$. The syntax of modal logic formulae is defined by the grammar:

$$\varphi \ ::= \ q \mid \neg q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Box \varphi \mid \Diamond \varphi$$

Modal Dependence Logic

Syntax of Modal Dependence Logic

Let AP be a set of atomic propositions and $p_1, \ldots, p_n, q \in AP$. The syntax of modal logic formulae is defined by the grammar:

$$\varphi ::= q \mid \neg q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Box \varphi \mid \Diamond \varphi \mid =\!(p_1, \ldots, p_n; q) \mid \neg =\!(p_1, \ldots, p_n; q)$$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$$W, T \models p \qquad \text{iff} \qquad p \in \pi(s) \text{ for all } s \in T$$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$$
\begin{array}{lll}
W, T \models p & \text{iff} & p \in \pi(s) \text{ for all } s \in T \\
W, T \models \neg p & \text{iff} & p \notin \pi(s) \text{ for all } s \in T
\end{array}
$$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$W, T \models p$	iff	$p \in \pi(s)$ for all $s \in T$
$W, T \models \neg p$	iff	$p \notin \pi(s)$ for all $s \in T$
$W, T \models \varphi \vee \psi$	iff	there are sets $T_1, T_2 \subseteq T$ with $T_1 \cup T_2 = T$, $W, T_1 \models \varphi$ and $W, T_2 \models \psi$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$W, T \models p$	iff	$p \in \pi(s)$ for all $s \in T$
$W, T \models \neg p$	iff	$p \notin \pi(s)$ for all $s \in T$
$W, T \models \varphi \vee \psi$	iff	there are sets $T_1, T_2 \subseteq T$ with $T_1 \cup T_2 = T$, $W, T_1 \models \varphi$ and $W, T_2 \models \psi$
$W, T \models \varphi \wedge \psi$	iff	$W, T \models \varphi$ and $W, T \models \psi$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$W, T \models p$	iff	$p \in \pi(s)$ for all $s \in T$
$W, T \models \neg p$	iff	$p \notin \pi(s)$ for all $s \in T$
$W, T \models \varphi \vee \psi$	iff	there are sets $T_1, T_2 \subseteq T$ with $T_1 \cup T_2 = T$, $W, T_1 \models \varphi$ and $W, T_2 \models \psi$
$W, T \models \varphi \wedge \psi$	iff	$W, T \models \varphi$ and $W, T \models \psi$
$W, T \models \Box \varphi$	iff	$W, \{s' \mid \exists s \in T \text{ s.t.} (s, s') \in R\} \models \varphi$

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$W, T \models p$	iff	$p \in \pi(s)$ for all $s \in T$
$W, T \models \neg p$	iff	$p \notin \pi(s)$ for all $s \in T$
$W, T \models \varphi \vee \psi$	iff	there are sets $T_1, T_2 \subseteq T$ with $T_1 \cup T_2 = T$, $W, T_1 \models \varphi$ and $W, T_2 \models \psi$
$W, T \models \varphi \wedge \psi$	iff	$W, T \models \varphi$ and $W, T \models \psi$
$W, T \models \Box \varphi$	iff	$W, \{s' \mid \exists s \in T \text{ s.t.} (s, s') \in R\} \models \varphi$
$W, T \models \Diamond \varphi$	iff	there is a set $T' \subseteq T$ s. t. $W, T' \models \varphi$ and for all $a \in T$ there is an $a' \in T'$ with $(a, a') \in R$.

Modal Logic

Semantics of Modal Logic

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ a set of initial states, and φ an ML formula and $p \in AP$. Inductive over the structure of φ we define

$W, T \models p$	iff	$p \in \pi(s)$ for all $s \in T$
$W, T \models \neg p$	iff	$p \notin \pi(s)$ for all $s \in T$
$W, T \models \varphi \vee \psi$	iff	there are sets $T_1, T_2 \subseteq T$ with $T_1 \cup T_2 = T$, $W, T_1 \models \varphi$ and $W, T_2 \models \psi$
$W, T \models \varphi \wedge \psi$	iff	$W, T \models \varphi$ and $W, T \models \psi$
$W, T \models \Box \varphi$	iff	$W, \{s' \mid \exists s \in T \text{ s.t.} (s, s') \in R\} \models \varphi$
$W, T \models \Diamond \varphi$	iff	there is a set $T' \subseteq T$ s. t. $W, T' \models \varphi$ and for all $a \in T$ there is an $a' \in T'$ with $(a, a') \in R$.

Modal Dependence Logic

Semantics of the Dependence Atom

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ the evaluation team. Let $p_1, \ldots, p_n, q \in AP$. Then $=(p_1, \ldots, p_n; q)$ is called a dependence atom. The truth of the dependence atom on W, T is defined by

Modal Dependence Logic

Semantics of the Dependence Atom

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ the evaluation team. Let $p_1, \ldots, p_n, q \in AP$. Then $=(p_1, \ldots, p_n; q)$ is called a dependence atom. The truth of the dependence atom on W, T is defined by

Modal Dependence Logic

Semantics of the Dependence Atom

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ the evaluation team. Let $p_1, \ldots, p_n, q \in AP$. Then $=(p_1, \ldots, p_n; q)$ is called a dependence atom. The truth of the dependence atom on W, T is defined by

$$W, T \models \;=(p_1, \ldots, p_n; q) \quad \text{iff} \quad \text{for all } s_1, s_2 \in T \text{ it holds that}$$
$$\pi(s_1) \cap \{p_1, \ldots, p_n\} \neq \pi(s_2) \cap \{p_1, \ldots, p_n\}$$
$$\text{or } \pi(s_1) \cap \{q\} = \pi(s_2) \cap \{q\}$$

Modal Dependence Logic

Semantics of the Dependence Atom

Let $W = (S, R, \pi)$ an AP-Kripke structure, $T \subseteq S$ the evaluation team. Let $p_1, \ldots, p_n, q \in AP$. Then $=(p_1, \ldots, p_n; q)$ is called a dependence atom. The truth of the dependence atom on W, T is defined by

$$W, T \models \; =(p_1, \ldots, p_n; q) \quad \text{iff} \quad \text{for all } s_1, s_2 \in T \text{ it holds that } \pi(s_1) \cap \{p_1, \ldots, p_n\} \neq \pi(s_2) \cap \{p_1, \ldots, p_n\} \text{ or } \pi(s_1) \cap \{q\} = \pi(s_2) \cap \{q\}$$

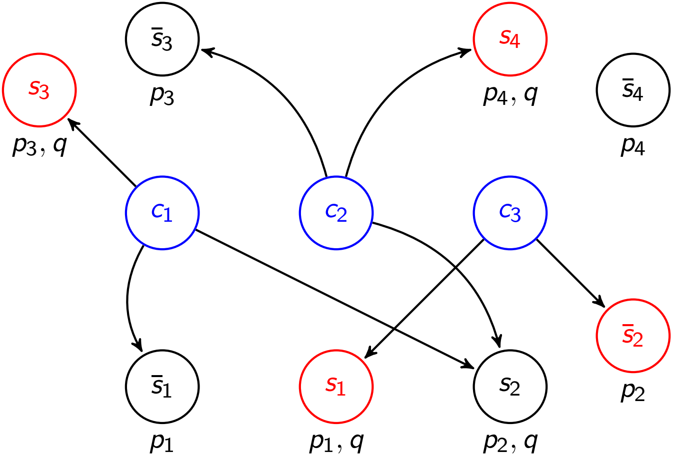
$$W, T \models \; \neg =(p_1, \ldots, p_n; q) \quad \text{iff} \quad T = \emptyset$$

Modal Dependence Logic

Example: Let $\varphi := \Diamond =\!(p_1, \ldots, p_4; q)$ and $T := \{c_1, c_2, c_3\}$.

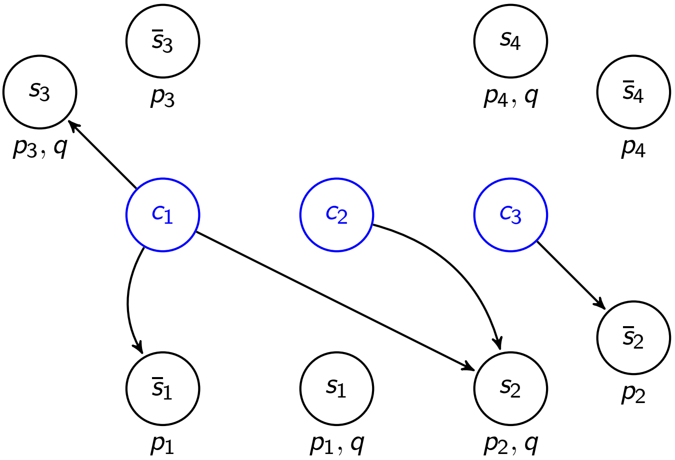
Modal Dependence Logic

Example: Let $\varphi := \Diamond {=}(p_1, \ldots, p_4; q)$ and $T := \{c_1, c_2, c_3\}$.



Modal Dependence Logic

Example: Let $\varphi := \Diamond =(p_1, \ldots, p_4; q)$ and $T := \{c_1, c_2, c_3\}$.



Model Checking

Model Checking is a formal method to verify a given formula.

Model Checking

Model Checking is a formal method to verify a given formula.

The Model Checking problem

Let $M \subseteq \{\Box, \Diamond, \wedge, \vee, \neg, =\}$.
Given: A Kripke structure $W = (S, R, \pi)$, a formula $\varphi \in \mathrm{MDL}(M)$ and an evaluation team $T \subseteq S$.
Problem: Check, whether $W, T \models \varphi$.

Model Checking

Model Checking is a formal method to verify a given formula.

The Model Checking problem

Let $M \subseteq \{\Box, \Diamond, \wedge, \vee, \neg, =\}$.
Given: A Kripke structure $W = (S, R, \pi)$, a formula $\varphi \in \mathrm{MDL}(M)$ and an evaluation team $T \subseteq S$.
Problem: Check, whether $W, T \models \varphi$.

$$\text{MDL-MC}(M) := \left\{ \langle W, T, \varphi \rangle \;\middle|\; \begin{array}{l} W = (S, R, \pi) \text{ an } AP\text{-Kripke structure}, \\ T \subseteq S, \varphi \in \mathrm{MDL}(M) \text{ and } W, T \models \varphi \end{array} \right\}.$$

Complexity Results on MDL-MC

Complexity Results on MDL-MC

Theorem

Model checking for modal dependence logic is NP-complete.

Complexity Results on MDL-MC

Theorem

Model checking for modal dependence logic is NP-complete.

We have to show:

Complexity Results on MDL-MC

Theorem

Model checking for modal dependence logic is NP-complete.

We have to show:

- MDL-MC is in NP

Complexity Results on MDL-MC

Theorem

Model checking for modal dependence logic is NP-complete.

We have to show:

- MDL-MC is in NP
- MDL-MC is NP-hard

The MDL Model Checking problem is in NP

Algorithm

```
bool check(W = (S, R, π), φ, T)
  case φ
  when φ = p
    foreach s_i ∈ T
      if not p ∈ π(s_i) then
        return false;
    return true;
  when φ = ¬p
    foreach s_i ∈ T
      if p ∈ π(s_i) then
        return false;
    return true;
```

The MDL Model Checking problem is in NP

Algorithm

```
when φ = ψ ∨ θ
  guess two sets A, B ⊆ T;
  if not A ∪ B = T then
    return false;
  return (check (W, ψ, A) and check (W, θ, B));
when φ = ψ ∧ θ
  return (check (W, ψ, T) and check (W, θ, T));
```

The MDL Model Checking problem is in NP

Algorithm

when $\varphi = \Diamond\psi$
  guess set of states T' ;
  foreach $s \in T$
    if there is no $s' \in T'$ with $(s, s') \in R$ then
      return false;
  return check (W, ψ, T');
when $\varphi = \Box\psi$
  $T' := \emptyset$;
  foreach $s' \in S$
    foreach $s \in T$
      if $(s, s') \in R$ then
        $T' \leftarrow T' \cup \{s'\}$
  return check (W, ψ, T');

The MDL Model Checking problem is in NP

Algorithm

```
when φ = =(p_1, ..., p_n; q)
  foreach (s, s') ∈ T × T
    if π(s) ∩ {p_1, ..., p_n} = π(s') ∩ {p_1, ..., p_n} then
      if not π(s) ∩ {q} = π(s') ∩ {q}
        return false;
  return true;

when φ = ¬=(p_1, ..., p_n; q)
  return T = ∅
```

The MDL Model Checking problem is NP-hard

Proposition

MDL-MC is NP-hard.

The MDL Model Checking problem is NP-hard

Proposition

MDL-MC is NP-hard.

We reduce 3SAT onto MDL-MC, i.e. for every 3SAT formula ϕ, we find an instance of MDL-MC which is at least as hard as ϕ.

Complexity Results

Operators					Complexity
$\vee$	$\wedge$	$\Box$	$\Diamond$	$=(\cdot)$	
$+$	$+$	$*$	$*$	$+$	NP-complete
$*$	$*$	$*$	$+$	$+$	NP-complete
$+$	$*$	$+$	$*$	$+$	NP-complete
$-$	$*$	$*$	$-$	$*$	in P
$+$	$-$	$-$	$-$	$+$	in NP

Complexity Results with bounded $=(\cdot)$

Operators					Complexity
$\vee$	$\wedge$	$\Box$	$\Diamond$	$=(\cdot)$	
$+$	$+$	$*$	$*$	$+$	NP-complete
$+$	$*$	$*$	$+$	$+$	NP-complete
$*$	$+$	$*$	$+$	$+$	NP-complete
$+$	$*$	$+$	$*$	$+$	NP-complete
$-$	$-$	$*$	$*$	$*$	in P
$-$	$*$	$*$	$-$	$*$	in P
$*$	$-$	$-$	$-$	$*$	in P

We limit the arity of the dependence atom, i.e. all dependence atoms are of the form $=(p_1, \ldots, p_j; q)$ where $j < k$ with a fixed $k \in \mathbb{N}$.

Complexity Results with bounded $=(\cdot)$

Operators					Complexity
$\vee$	$\wedge$	$\Box$	$\Diamond$	$=(\cdot)$	
$+$	$+$	$*$	$*$	$+$	NP-complete
$+$	$*$	$*$	$+$	$+$	NP-complete
$*$	$+$	$*$	$+$	$+$	NP-complete
$+$	$*$	$+$	$*$	$+$	NP-complete
$-$	$-$	$*$	$*$	$*$	in P
$-$	$*$	$*$	$-$	$*$	in P
$*$	$-$	$-$	$-$	$*$	in P

We limit the arity of the dependence atom, i.e. all dependence atoms are of the form $=(p_1, \ldots, p_j; q)$ where $j < k$ with a fixed $k \in \mathbb{N}$.

Open Questions

- MDL-MC($\{\neg, \vee, =(\cdot)\}$) NP-complete?

Open Questions

- MDL-MC($\{\neg, \vee, =(\cdot)\}$) NP-complete?
- Classification for DCTL-MC?

Open Questions

- MDL-MC($\{\neg, \vee, =(\cdot)\}$) NP-complete?
- Classification for DCTL-MC?
- Open case for MDL-MC($\Diamond, \wedge, =(\cdot)$) with bounded dependence atom, is solved for $k \geq 0$.

Open Questions

- MDL-MC($\{\neg, \vee, =(\cdot)\}$) NP-complete?
- Classification for DCTL-MC?
- Open case for MDL-MC($\Diamond, \wedge, =(\cdot)$) with bounded dependence atom, is solved for $k \geq 0$.

Thank you!